Definition 1. Let V be a vector space over $\mathbf{F}_q$. Then a set of vectors $A = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ in V is said to be *linearly independent* if and only if a *linear combination* $\lambda_1\mathbf{v}_1 + \cdots + \lambda_k\mathbf{v}_k$ being a zero-vector implies that λ_i, $i = 1, \ldots, k$, are zero.

Definition 2. Let V be a vector space over $\mathbf{F}_q$. Let $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a non-empty subset of V. Then, the *linear span* $\langle S \rangle$ of S is defined as

$$\langle S \rangle = \left\{ \sum_{i=1}^{k} \lambda_i \mathbf{v}_i : \lambda_i \in \mathbf{F}_q \right\}$$

We say that the span $\langle S \rangle$ of S is a subset of V generated or spanned by S. Let C be a subspace of V, then a subset S of C is called a *generating*- or *spanning set* of C if $C = \langle S \rangle$.

Definition 3. An *inner product* on $\mathbf{F}_q$ is a mapping $\langle \mathbf{a}, \mathbf{b} \rangle : \mathbf{F}_q^n \times \mathbf{F}_q^n \to \mathbf{F}_q$ such that, for all $\mathbf{u}, \mathbf{v}, \mathbf{w}$ in $\mathbf{F}_q^n$,

a. $\langle \mathbf{u} + \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle$

b. $\langle \alpha \mathbf{v}, \mathbf{w} \rangle = \alpha \langle \mathbf{v}, \mathbf{w} \rangle$, where α is a scalar

c. $\langle \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{w}, \mathbf{v} \rangle$

d. $\langle \mathbf{u}, \mathbf{v} \rangle = 0$, for all non-zero $\mathbf{u}$ in $\mathbf{F}_q^n$, if and only if $\mathbf{v} = \mathbf{0}$

Definition 4. Let $\mathbf{v}$ and $\mathbf{w}$ be two vectors in $\mathbf{F}_q^n$. Then the *scalar product*, aka the *dot-* or *Euclidean inner product*, between $\mathbf{v}$ and $\mathbf{w}$ is defined as $\mathbf{v} \cdot \mathbf{w} = \sum_{i=1}^n v_i w_i \in \mathbf{F}_q$. The two vectors are said to be *orthogonal* to each other if and only if $\mathbf{v} \cdot \mathbf{w} = 0$. The *orthogonal complement* $S^\perp$ of a non-empty subset S of $\mathbf{F}_q^n$, is defined to be

$$S^\perp = \left\{ \mathbf{v} \in \mathbf{F}_q^n : \mathbf{v} \cdot \mathbf{s} = 0 \,\text{for all}\, \mathbf{s} \in S \right\}$$

When $S = \emptyset$ we define $S^\perp = \mathbf{F}_q^n$.

Note 1. The orthogonal complement $S^{\perp}$ of a non-empty subset S of a vector space $\mathbf{F}_q^n$ is always a subspace of $\mathbf{F}_q^n$. Moreover, $\langle S\rangle^{\perp} = S^{\perp}$.

Definition 5. Let V be a vector space over $\mathbf{F}_q$. Then a non-empty subset $A = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ of V is called a *basis* for V if $V = \langle A \rangle$ and A is linearly independent.

Theorem 1. Let V be a vector space over $\mathbf{F}_q$. If $\dim v = k$, then V has q^k elements and

$$\frac{1}{k!}\prod_{i=0}^{k-1}\left(q^k - q^i\right)$$

different bases.

Proof. If the basis for V is $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ and $\lambda_1, \ldots, \lambda_k$ are in $\mathbf{F}_q$, then $V = \sum_{i=1}^{k} \lambda_i \mathbf{v}_i$. Since $|\mathbf{F}_q|$ is q, there are q choices for each λ_i. Therefore V has exactly q^k elements.

Let $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a basis for V. Since B is non-empty, $\mathbf{v}_1 \neq \mathbf{0}$ and there are $q^k - 1$ choices for $\mathbf{v}_1$. Then there are $q^k - q^{i-1}$ choices of $\mathbf{v}_i$, for $i = 2, \ldots, k$ because $\mathbf{v}_i \notin \langle \mathbf{v}_1, \ldots, \mathbf{v}_{i-1} \rangle$. Therefore there are $\prod_{i=0}^{k-1} (q^k - q^i)$ distinct ordered k-tuples, $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$. The order of $\mathbf{v}_1, \ldots, \mathbf{v}_k$ is irrelevant, hence the number of distinct bases for V is $\frac{1}{k!} \prod_{i=0}^{k-1} (q^k - q^i)$.

Corollary 1[1]. Let C be a linear code of length n over $\mathbf{F}_q$. Then, $\dim C = \log_q |C|$, in other words $|C| = q^{\dim C}$.

Theorem 2. Let S be a subset of $\mathbf{F}_q^n$. Then, $\dim \langle S \rangle + \dim S^\perp = n$.

Proof. When $\langle S \rangle = \{\mathbf{0}\}$, this is obvious. Next, consider cases where $\dim \langle S \rangle = k$, where $1 \le k < n$. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a basis of $\langle S \rangle$, then we need to show that $\dim S^\perp = \dim \langle S \rangle^\perp = n-k$. Since $\mathbf{x}$ is in $S^\perp$ if and only if $\mathbf{v}_1 \cdot \mathbf{x} = \cdots = \mathbf{v}_k \cdot \mathbf{x} = 0$, or equivalently $A\mathbf{x} = \mathbf{0}$, where the $k \times n$ matrix A is

$$A = \begin{bmatrix} \mathbf{v}_1^T \\ \vdots \\ \mathbf{v}_k^T \end{bmatrix}$$

we know that the rows of A are linearly independent. Then $A\mathbf{x} = \mathbf{0}$ is a linear system of k linearly independent equations in n variables, where $n > k$, and therefore admits a solution space of dimension $n - k$. ¶

Corollary 2[2]. Let C be a linear code of length n over $\mathbf{F}_q$. Then $C^\perp$ is also a linear code, and $\dim C + \dim C^\perp = n$

Proof. This follows from Note 1 and Theorem 2 above. ¶

Theorem 3. Let C be a linear code of length n over $\mathbf{F}_q$. Then, $(C^\perp)^\perp = C$.

Proof. From Corollary 2[2], we have $\dim C + \dim C^\perp = n$ and $\dim C^\perp + \dim (C^\perp)^\perp = n$, and hence $\dim C = \dim (C^\perp)^\perp$. Let $\mathbf{c}$ be in C. Then for all $\mathbf{x}$ in C, we have $\mathbf{c} \cdot \mathbf{x} = 0$, hence $C \subseteq (C^\perp)^\perp$ and the proof. ¶

Definition 6. A *linear code* of length n over $\mathbf{F}_q$ is a subspace of $\mathbf{F}_q^n$. The *dual code* $C^\perp$ of C is the orthogonal complement of the subspace C of $\mathbf{F}_q^n$. The *dimension* of the linear code C is the dimentions of C as a vector space over $\mathbf{F}_q$, that is to say, $\dim C$. A linear code C of length n and dimension k over $\mathbf{F}_q^n$ is called a q-ary $[n, k]$-code, or an (n, q^k)-linear code. If the distance d of C is known, it is called an $[n, k, d]$-linear code. Furthermore, C is said to be *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$.

Definition 7. Let $\mathbf{x}$ be a word in $\mathbf{F}_q^n$. Then, the *Hamming weight* $w(\mathbf{x})$ of $\mathbf{x}$ is defined as the number of non-zero letters in $\mathbf{x}$. In other words, $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$, where $\mathbf{0}$ is the zero word and $d(\mathbf{x}, \mathbf{y})$ is the Hamming distance between two words $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{F}_q^n$. For each element x of $\mathbf{F}_q$, the Hamming weight may be defined as

$$w(x) = d(x, 0) = \begin{cases} 1, & \text{if } x \neq 0 \\ 0, & \text{if } x = 0 \end{cases}$$

Then for $\mathbf{x} = (x_1, \ldots, x_n)$ in $\mathbf{F}_q^n$,

$$w(\mathbf{x}) = w(x_1) + \cdots + w(x_n)$$

Theorem 4. Let $\mathbf{x}$ and $\mathbf{y}$ be two words in $\mathbf{F}_q^n$. Then $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$.

Proof. For each pair of letters x and y in $\mathbf{F}_q$, we know that $d(x, y) = 0$ if and only if $x = y$, that is if and only if $x - y = 0$, or equivalently $w(x - y) = 0$. The proof follows since $w(\mathbf{x}) = \sum_{i=1}^n w(x_i)$ and $d(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n d(x_i, y_i)$. ¶

Corollary 4[3]. Let q be an even positive integer. Then, for any two words $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{F}_q^n$ we have $d(\mathbf{x},\mathbf{y}) = w(\mathbf{x}+\mathbf{y})$.

Proof. The proof follows from the fact that $a = -a$ for all a in $\mathbf{F}_q$ when q is even. ¶

Theorem 5. Let $\mathbf{x}$ and $\mathbf{y}$ be two words in $\mathbf{F}_2^n$. Then, $w(\mathbf{x})+w(\mathbf{y}) \geq w(\mathbf{x}+\mathbf{y})$.

Proof. For $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ in $\mathbf{F}_q^n$, let

$$\mathbf{x} * \mathbf{y} = (x_1 y_1, \ldots, x_n y_n)$$

Then, for $q = 2$ and $n = 1$,

x	y	$x * y$	$w(x) + w(y) - 2w(x * y)$	w(x+y)
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	0	0

From this together with Definition 7 we know that

$$w(\mathbf{x} + \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} * \mathbf{y})$$

for $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{F}_2$, and thus the proof is implied. ¶

Problem 1. Prove for any prime power q and $\mathbf{x}, \mathbf{y}$ in $\mathbf{F}_q^n$, that

$$w(\mathbf{x}) + w(\mathbf{y}) \geq w(\mathbf{x} + \mathbf{y}) \geq w(\mathbf{x}) - w(\mathbf{y})$$

Definition 8. Let A be a matrix over $\mathbf{F}_q$. An *elementary row operation* performed on A is any one among the following.

a. interchange of two rows
b. multiplication of a row by a non-zero scalar
c. replacement of a row by its summation with a scalar multiple of another row

Two matrices are said to be *row equivalent* to each other if one is obtainable from another by a sequence of elementary row operations.

Definition 9. Any matrix is row equivalent to a matrix in *row echelon* (RE) form or *reduced row echelon* (RRE)† form formed by a sequence of elementary row operations done upon itself. The RRE form of any given matrix is unique, but its RE's may not be so.